埼玉女子短期大学研究紀要　第３号　1992.03

ゼロ知識対話証明と本人確認

Zero-knowledge Interactive Proof and Identification

高　林　茂　樹
Shigeki Takabayashi

The system based on Zero-knowledge Interactive Proof must be expanded by IC-card. A part of large scale secret number is inputed into IC-card and calculation starts. The inputed data had better be erased after about 5 minutes.

１．はじめに

ゼロ知識対話証明は、パスワード（暗証番号）などの本人の秘密を相手に漏らすことなく、本人が正しいパスワードを知っていることを相手に証明する方法である。今日の情報化社会において、キャッシュカードによる銀行での現金の引出し、クレジットカードによる店での買い物や電話での通信販売などの取り引きで不正防止のため暗証番号等により本人確認がされている。しかしながら、このような場面で、暗証番号を入力する時あるいは相手に伝える時に、見られたり、聞かれたり、通信途中で漏れたりして不正使用が行われないとは限らない。ゼロ知識対話証明が利用できるようになれば暗証番号などの秘密を相手に示すことなく対話形式で本人確認が可能になる。

ゼロ知識対話証明は、大きな数の素因数分解がむずかしいという公開鍵暗号理論と同じ考えを利用したものである。[1] 暗号理論を使用し、パスワードを暗号化して相手に送っても相手は暗号を解読するので、相手にはパスワードはわかってしまうがゼロ知識対話証明ではそのように相手にわかることもなくなる。大きな数として、最新の高性能コンピュータで素因数分解の計算をしても数百年以上の時間を要する数を使用する必要があるが、ゼロ知識対話証明による本人確認では、本人以外の人がパスワード等の秘密を知ることは不可能と言える。

ゼロ知識対話証明は、1985年 Goldwasser 教授、Micali 教授、Rackoff 教授の連名で発表された。しかしながら、この実用化については、ベルギーやイギリスの企業でＩＣカード化して使われていると言われるが、ＩＣカード内にパスワードや計算ロジックが組み込まれているため紛失などで他人に渡ってしまうと不正使用の可能性が大きい。[2] こ

のように実用化に関してはまだ多くの問題が残されている。本論文では、ゼロ知識対話証明の本人確認についての問題点を整理するとともに解決方法について考察する。

２．コンピュータと本人確認

２－１．本人確認の現状

コンピュータを利用する本人確認では、現在次のものが使用されている。[3]

①　パスワード

暗証番号とも言い最も一般的なものである。パスワードが提示されると、前もってコンピュータに登録されているものと比較し一致した場合、本人であると確認される。故意または偶然にパスワードがわかってしまうと不正使用される危険がある。

②　所有物

磁気カード、ＩＣカード、光カードなどを持っている人を本人であると確認する。パスワードと併用されることが多い。ＩＣカードの中には、いちいち取り出して提示しなくとも済む無線式のものも開発されている。

③　行　動

署名が代表的なものである。これでは署名パターン（筆跡）の特徴を抽出して、前もって登録されているものと比較し一致した場合、本人であると確認される。

④　身体的特徴

指紋、掌紋、手形（指の長さなど）、網膜血管パターンなどの特徴を抽出して、前もって登録されているものと比較し一致した場合、本人であると確認される。

パスワードには漏洩の危険、所有物には紛失の危険がある。署名（筆跡）は、人による違いはあるものの時間経過による字体の変化、模倣の危険なども存在する。身体的特徴は時間経過や外傷、病気などによる変化で本人確認ができなくなることもある。

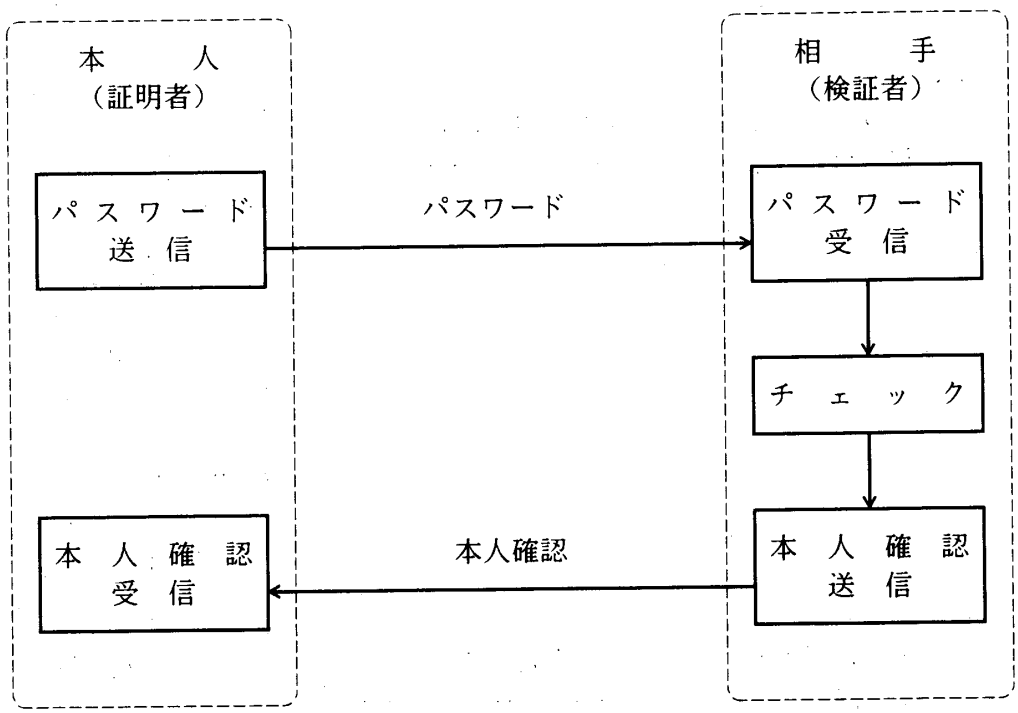
２－２．ゼロ知識対話証明の方法

パスワード使用により本人確認する場合、漏洩の危険を避けるためいろいろな方法が考えられる。パスワードによる本人確認を次の３つに分類する。

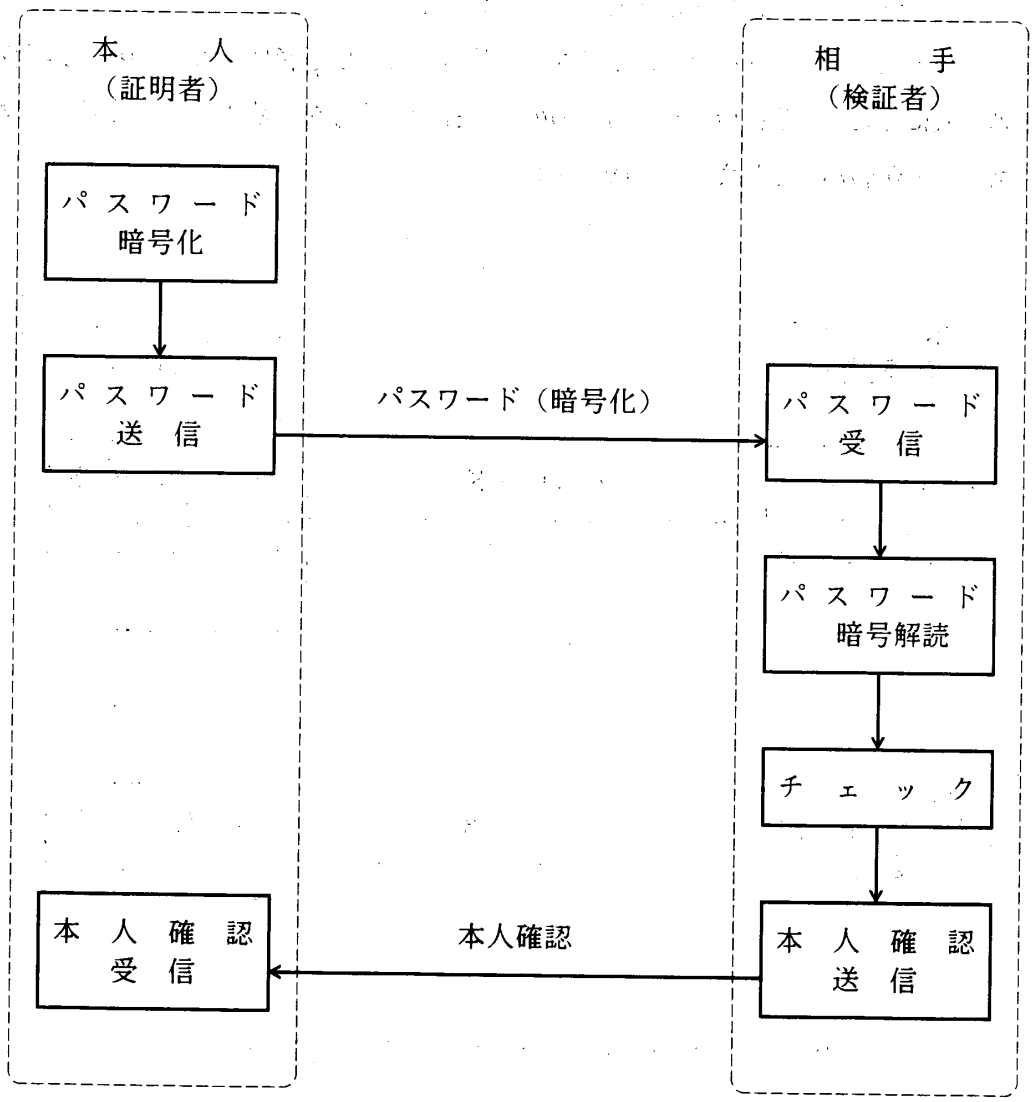
①　証明者（本人）はパスワードそのものを検証者（相手）に示して本人であることを証明する。当然、検証者にはパスワードがわかってしまう。また途中で検証者以外の

人に見られたりして漏れることもある。（図－１）

② 証明者はパスワードそのものではなく、暗号化して検証者に送る。途中で検証者以外の人に漏れる危険は少なくなるものの、検証者は暗号を解読するので検証者にはパスワードがわかってしまう。（図－２）



図－１　パスワードによる本人確認（一般的）



図－２　パスワードによる本人確認（暗号化）

③　証明者はゼロ知識対話証明により、パスワードを検証者に知られることなく検証者に自分がパスワードを知っていることを伝える。

上記③のゼロ知識対話証明の代表的なものが次に述べるFiat−Shamir法である。[4]

（図－３）

証明者は、２つの素数ｐ，ｑからなる合成数ｎ（ｎ＝ｐ×ｑ）を公開する。それと秘密情報（パスワードなど）Ｓに対して$Z \equiv S^2 \pmod{n}$を満たすＺを公開する。

ここで証明者は、Ｓを公開することなくＳを知っていることを検証者に証明できればよい。

① 証明者は乱数Ｓを選ぶ。

$X \equiv R^2 \pmod{n}$ を計算して検証者に送る。

② 検証者は、0または1をランダムに選び証明者に送る。（これをｅとする）

$e \in \{0, 1\}$

③ 証明者は

ｅ＝0　の時は　Ｙ＝Ｒ　　を検証者に送る。

ｅ＝1　の時は　$Y \equiv ZR \pmod{n}$ を検証者に送る。

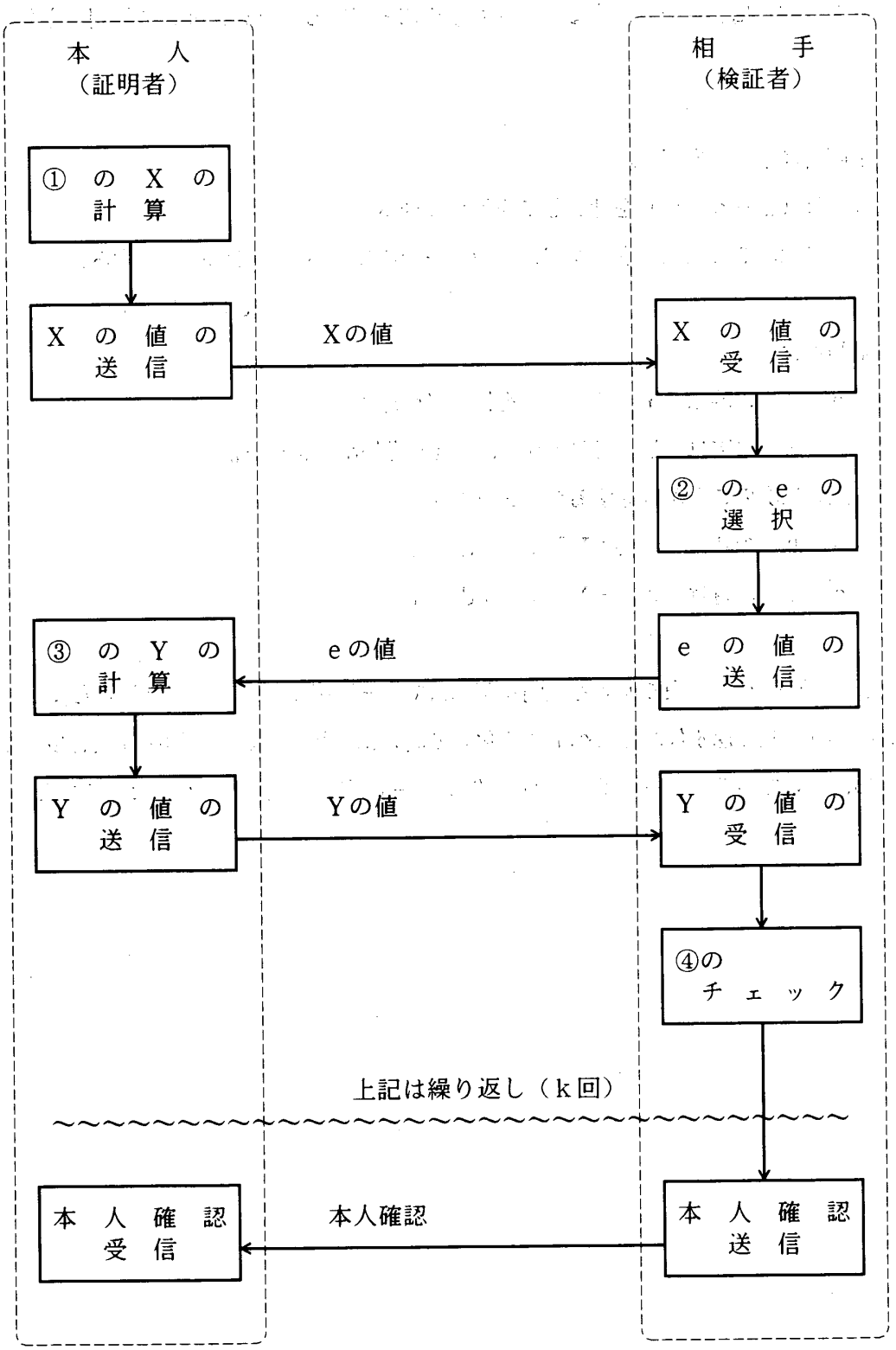
④ 検証者は次のことが成立するかチェックする。

ｅ＝0　の時は　$X \equiv Y^2 \pmod{n}$

ｅ＝1　の時は　$ZX \equiv Y^2 \pmod{n}$

上記の①～④をｋ回繰り返すと証明者が本人である確率は、$(1 - 2^{-K})$ となる。

このように繰り返す代わりにベトクル化して同時に実行することも通信回数を少なくするために有効である。表－1はn=151592003、S=911031で20回繰り返した例である。



図－３　パスワードによる本人確認（ゼロ知識対話証明）

表－１　ゼロ知識対話証明（例）

①の 乱数R	①の Xの値	②の eの値	③の Yの値	④の チェック（Y^2）
85725	72359481	0	85725	72359481
92259	22570913	1	68839367	115650862
14024	45080573	1	42570492	17377769
6489	42107121	0	6489	42107121
25123	24797117	1	149031363	68303841
25003	18781997	1	39707643	10404677
11991	143784081	0	11991	143784081
41944	91787103	1	11099508	105411961
19550	79018494	1	74391699	43042480
1059	1121481	0	1059	1121481
41550	58890467	1	106929303	49573840
96100	139689820	0	96100	139689820
20959	136095675	1	145298354	88495322
71206	67758337	1	141088105	29978941
2310	5336100	0	2310	5336100
69738	12444548	1	16430621	110839040
78179	48275921	1	126843142	148595851
84664	43168755	1	122791060	7169588
93880	21118226	1	29700588	147464528
10906	118940836	0	10906	118940836

n=151592003 (p=19583, q=7741)　S=911031　Z=11266536　k=20

３．実用化に向けて

３－１．問題点

ゼロ知識対話証明は一部で使われ始めたと言うもののまだ多くの問題が残されている。主な問題点を整理すると次のようになる。

①　計算量

数値の桁数が秘密を保持するためにはある程度以上（２００桁程度）大きいことが必要となる。そのため証明者はその計算を暗算で行うことは通常無理である。検証者側でも同程度の計算が必要である。

②　信頼性

証明者が事前に検証者から送られて来るｅの値（０または１）を予想してＸを送ることによりそれが的中すればｋ回の繰り返しでは2^{-k}の確率で本人で無いこともある。

３－２．解決策

計算量に関しては、暗算の達人なら可能性としては考えられないこともないが、一般には証明者側に小型のコンピュータが必要となる。したがってコンピュータ利用を前提とした解決策について考察する。

（１）ＩＣカードに秘密情報と計算手順を組み込む

証明者側はＩＣカードを用いて計算することが可能で、先に述べたようにベルギーなどで使われている。しかしながら、この場合はＩＣカードの中に秘密情報であるパスワードと計算手順がすべて組み込まれている。したがってこのＩＣカードを紛失して他人に渡るとそのまま使用されてしまう危険がある。

検証者側もコンピュータを必要とするが、検証者側が移動することはあまりないと考えられるのでその場合はＩＣカードでなくともよく、パソコンや計算センターの利用も可能である。

証明者側がＩＣカードを使う場合、危険を少なくするため次のような制約を付けることも考えられる。

① 利用場所の限定

自宅あるいは会社など限られた範囲の電話機にＩＣカードの読み取り装置を付けて使用する。紛失の危険の少ない所での使用ならすぐにでも可能である。

② ＩＣカード起動用パスワード

ＩＣカードの計算を開始させるために人の記憶できる程度（４桁程度）のパスワードを入力する。このパスワードは入力してから５分間程度有効になるようにし、その後自動的に消去する。このようにすることにより事前にパスワードの入力ができ人に見られて漏洩する危険が少なくなる。

（２）ＩＣカードに計算手順を組込む（秘密情報は無しまたは一部組込む）

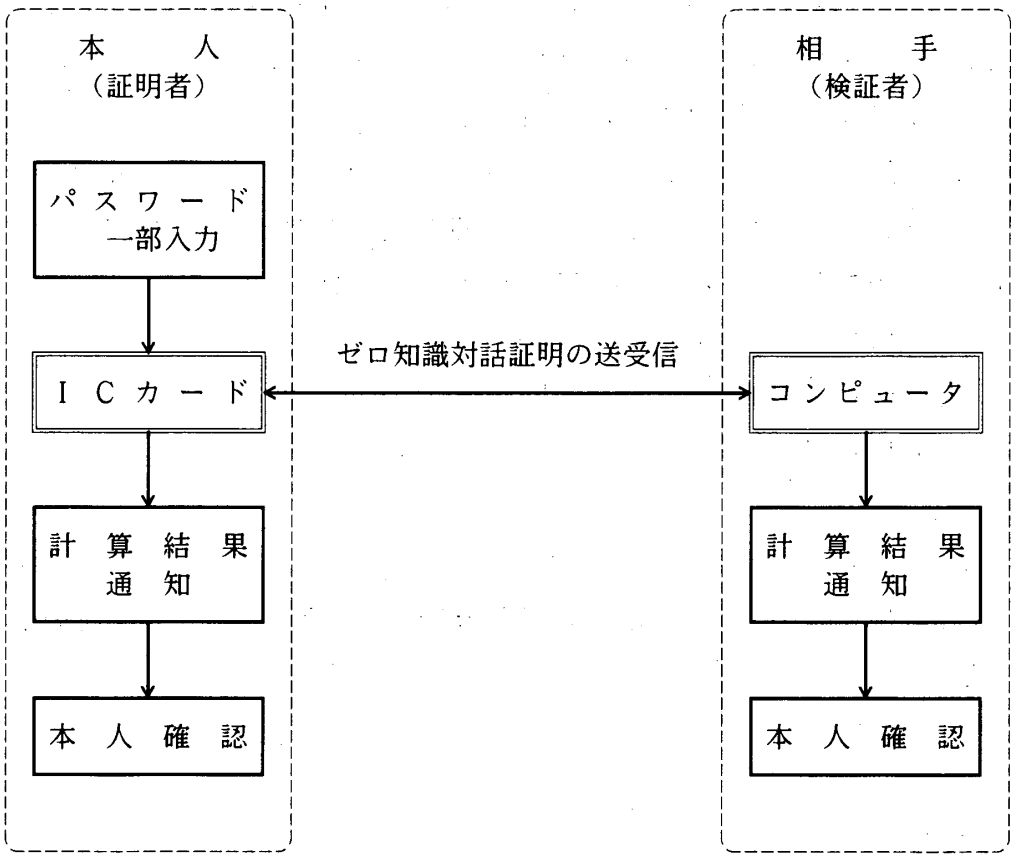
① パスワードの短縮

ＩＣカードに短縮したパスワードを、使用する時点で入れて計算させる。この場合ｎも大きくできないので、ｎが素因数分解されてしまう危険がある。

② パスワードの一部組込み

パスワード全部ではなく一部をＩＣカードに記憶しておき、残りの部分は使用する

ときに入れて計算させる。この場合（１）の②と同様にパスワードは入力してから５分間程度有効になるようにしその後消去する。パスワードのすべてがＩＣカード内に無いだけ（１）の②より安全性は高い。（図－４）



図－４　ＩＣカード使用のゼロ知識対話証明（例）

ＩＣカード利用では（２）の②の方法が現実性、安全性から見てよいのではないかと思われる。Ｚ，ｎはカードを発行できるセンターのような所で計算しておく必要がある。

問題点の②については繰り返し回数を検証者側で重要度に応じて決めることも可能である。繰り返し回数が多ければ指数級数的に信頼度が増加する。

４．おわりに

コンピュータ利用が進むにしたがって、本人確認の方法も様々なものが現れ生活を便利にしてきた一方で悪用による被害も発生している。クレジット電話での被害も報道されているが、現在の４桁の暗証番号を入れるだけで不正使用を完全に防止することは困難である。現段階では、少なくとも計算機能の組み込まれたＩＣカードがなくてはできないが、今後は、もっと小さくて常に身につけておくことのできるものに計算機能を組み込むなど、より安全で実用的な本人確認のシステムを確立していく必要がある。

このゼロ知識対話証明は本人の秘密を自分以外にまったく漏らすこと無くその人が「私はその秘密を確かに知っている」と言うことを証明できるので様々な応用が考えられている。たとえば次のプロトコルの安全性確認のためには不可欠のものである。[5]

① 電話によるコイン投げやじゃんけん

② お互いの財産額は秘密にしての財産比べ

③ 通信による無記名投票

このほかにも今後コンピュータ利用により情報が数値化され、データベース化されるとプライバシー保護や安全性の面からゼロ知識対話証明の応用範囲が広がっていくのではないかと思う。

（参考文献）

(1) 辻井重男、笠原正雄、暗号と情報セキュリティ、１９９０

(2) 小山謙二、ゼロ知識対話証明の原理と課題、情報処理、Vol.32 No.6 pp643−653 (1991.6)

(3) 宝木和夫、中村勤、暗号方式と応用、情報処理、Vol.32 No.6 pp714−723 (1991.6) (1991.6)

(4) 太田和夫、藤岡淳、ゼロ知識証明の応用、情報処理、Vol.32 No.6 pp654−661 (1991.6)

(5) 黒沢馨、岡本龍明、ゼロ知識証明とマルチパーティプロトコル、情報処理、Vol.32 No.6 pp663−671 (1991.6)